CLAIMS

We claim:

1. A method for applying personal information in the use of Web services comprising:

   a) eliciting an action by a user that verifies said user's identity,

   b) associating one or more pairs of user input sequences and URL's,

   c) connecting said pairs with said user's verified identity,

   d) storing said pairs connected with said user's identity in a database accessible on the public Internet,

   e) retrieving each of said pairs when a user input sequence included in a particular pair is needed by said user for entry at an associated URL included in said particular pair, and

   f) entering said user input sequence included in said particular pair into the Web page at said associated URL included in said particular pair,

   whereby said user can easily recall any repetitive personal information that said user needs to access and use Web services with minimal maintenance burden for said user.

2. The method of claim 1 wherein at least one of said pairs includes a type of user input sequence that is a sign-on procedure for a Web service.

3. The method of claim 1 wherein at least one of said pairs includes a type of user input sequence that is entry data for an order form for purchasing via a Web service.

4. The method of claim 1 wherein at least one of said pairs includes a recorded user input sequence that is captured by recording during effective use of said recorded user input sequence at the URL associated with said recorded user input sequence.

5. The method of claim 1 wherein at least one of said pairs is formed by direct entry of a predetermined user input sequence and a URL associated with said predetermined user input sequence.

6. The method of claim 1 wherein said action by said user that verifies said user's identity is

entry of a passphrase.

7. The method of claim 6 wherein said user's identity is further verified by checking data on a portable memory device possessed by said user.

8. The method of claim 6 wherein said user's identity is further verified by comparing one or more of the physical characteristics of said user to biometric data stored on a portable memory device possessed by said user.

9. A method for applying personal information in the use of Web services comprising:

   a) entry by a user of a passphrase that verifies said user's identity,

   b) encrypting said passphrase with one-way encryption to derive a User ID,

   c) associating one or more pairs of user input sequences and URL's,

   d) encrypting said pairs with a key derived from said passphrase,

   e) connecting the encrypted pairs with said User ID,

   f) storing said encrypted pairs connected with said User ID in a database accessible on the public Internet,

   g) retrieving each of said encrypted pairs when a user input sequence included in a particular encrypted pair is needed by said user for entry at an associated URL included in said particular encrypted pair,

   h) decrypting said particular encrypted pair with said key derived from said passphrase, and

   i) entering said user input sequence included in said particular encrypted pair into the Web page at said associated URL included in said particular encrypted pair,
   whereby said user can easily recall any repetitive personal information that said user needs to access and use Web services with minimal maintenance burden and a high degree of privacy for said user.

10. The method of claim 9 wherein at least one of said pairs includes a type of user input sequence that is a sign-on procedure for a Web service.

11. The method of claim 9 wherein at least one of said pairs includes a type of user input sequence that is entry data for an order form for purchasing via a Web service.

12. The method of claim 9 wherein at least one of said pairs includes a recorded user input sequence that is captured by recording during effective use of said recorded user input sequence at the URL associated with said recorded user input sequence.

13. The method of claim 9 wherein at least one of said pairs is formed by direct entry of a predetermined user input sequence and a URL associated with said predetermined user input sequence.

14. The method of claim 9 wherein said user's identity is further verified by checking data on a portable memory device possessed by said user.

15. The method of claim 9 wherein said user's identity is further verified by comparing one or more of the physical characteristics of said user to biometric data stored on a portable memory device possessed by said user.